ESA — 資料包捕獲和網路調查

目錄

簡介

本檔案介紹如何在思科電子郵件安全裝置(ESA)上設定和收集封包擷取，並執行其他網路調查和疑難排解。

背景資訊

當您聯絡思科技術支援遇到問題時，可能會要求您深入瞭解ESA的出站和入站網路活動。裝置能夠攔截和顯示通過裝置所連線的網路傳輸或接收的TCP、IP和其他資料包。您可能希望運行資料包捕獲以調試網路設定或驗證到達或離開裝置的網路流量。

> **附註**：本檔案所參考的軟體不是Cisco維護或支援的。此資訊出於方便而提供。如需更多幫助，請與軟體供應商聯絡。

必須注意的是，先前使用的 tcpdump CLI命令替換為新的 packetcapture 命令。此命令提供的功能與 tcpdump 命令時，也可用於GUI上。

如果運行AsyncOS版本6.x或更低版本，請參閱有關如何使用 tcpdump 本文檔的*Packet Captures on AsyncOS Versions 6.x and Everyers*部分中的命令。此外，*Packet Capture Filters*部分中描述的過濾器選項也適用於new packet capture命令。

AsyncOS 7.x及更高版本上的資料包捕獲

本節介紹AsyncOS 7.x及更高版本上的資料包捕獲過程。

啟動或停止資料包捕獲

若要從GUI啟動資料包捕獲，請導航到右上角的**幫助和支援**選單，選擇**Packet Capture**，然後按一下**Start Capture**。若要停止封包擷取程式，請按一下**「停止擷取」**。

附註：在GUI中開始的捕獲會在會話之間保留。

若要從CLI開始資料包捕獲，請輸入 **packetcapture > start** 指令。若要停止封包擷取程式，請輸入 **packetcapture > stop** 命令，會話結束時ESA會停止資料包捕獲。

封包擷取功能

以下是可用於操縱封包擷取的有用資訊清單：

- ESA將捕獲的資料包活動儲存到檔案中，並在本地儲存。您可以設定最大封包擷取檔案大小、封包擷取執行的時間長度，以及擷取執行所在的網路介面。您還可以使用過濾器將封包擷取限製為通過特定連線埠的流量或來自特定使用者端或伺服器IP位址的流量。
- 從GUI導航到**幫助和支援>資料包捕獲**，以檢視儲存的資料包捕獲檔案的完整清單。當運行資料包捕獲時，「資料包捕獲」頁顯示當前統計資訊（如檔案大小和所用時間）的捕獲狀態。
- 選擇捕獲並按一下**Download File**以下載儲存的資料包捕獲。
- 要刪除資料包捕獲檔案，請選擇一個或多個檔案，然後按一下**Delete Selected Files**。
- 若要使用GUI編輯資料包捕獲設定，請從「幫助和支援」選單中選擇**Packet Capture**，然後按一下**Edit Settings**。
- 要使用CLI編輯資料包捕獲設定，請輸入 **packetcapture > setup** 指令。

附註：GUI只顯示從GUI開始的資料包捕獲，而不顯示從CLI開始的資料包捕獲。同樣，CLI僅顯示從CLI開始的當前資料包捕獲的狀態。一次只能運行一個捕獲。

提示：有關資料包捕獲選項和過濾器設定的其他資訊，請參閱本文檔的**資料包捕獲過濾器**部分。要從GUI訪問AsyncOS聯機幫助，請導航到**幫助和支援>聯機幫助>搜尋資料包捕獲>**選擇**運行資料包捕獲。**

AsyncOS 6.x及更低版本上的資料包捕獲

本節介紹AsyncOS 6.x及更低版本上的資料包捕獲過程。

啟動或停止資料包捕獲

您可以使用 tcpdump 命令，以捕獲TCP/IP資料包和通過連線ESA的網路傳輸或接收的其他資料包。

完成以下步驟即可開始或停止封包擷取：

1. 輸入 **diagnostic > network > tcpdump** 命令。以下是輸出範例：

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. 設定介面（資料1、資料2或管理）和篩選器。

   附註：過濾器使用的格式與Unix tcpdump 指令。
3. 選擇START開始捕獲，選擇STOP結束捕獲。

   附註：捕獲正在進行時，請勿退出tcpdump選單。必須使用第二個CLI視窗來運行任何其他命令。捕獲過程完成後，必須從本地案頭使用安全複製(SCP)或檔案傳輸協定(FTP)從名為Diagnostic的目錄下載檔案(有關詳細資訊，請參閱*資料包捕獲過濾器*部分)。 這些檔案使用資料包捕獲(PCAP)格式，並可以使用Ethereal或Wireshark等程式進行檢視。

封包擷取過濾器

其 **Diagnostic > NET** CLI命令使用標準tcpdump過濾器語法。本節提供有關tcpdump捕獲過濾器的資訊並提供一些示例。

以下是所使用的標準篩選條件：

- **ip** — 所有IP通訊協定流量的過濾器
- **tcp** -所有TCP通訊協定流量的過濾器
- **ip host** -特定IP地址源或目標的過濾器

以下是一些使用中的篩選器的範例：

- **ip host 10.1.1.1** — 此過濾器捕獲包括10.1.1.1作為來源或目的地的任何流量。
- **ip host 10.1.1.1或ip host 10.1.1.2** — 此過濾器捕獲包含10.1.1.1或10.1.1.2作為源或目標的流量。

要檢索捕獲的檔案，請導航到**var > log > diagnostic**或**data > pub > diagnostic**以訪問Diagnostic目錄。

> **附註**：使用此命令時，可能會導致ESA磁碟空間耗盡，並且還會導致效能下降。思科建議您僅在思科TAC工程師的協助下使用此命令。

其他網路探查和調查

> **附註**：以下方法只能從CLI中使用。

TCPSERVICES

其 tcpservices 命令將顯示當前功能和系統進程的TCP/IP資訊。

```
example.com> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres     - Process for storing and querying quarantine data
  splunkd      - Processes for storing and querying Email Tracking data

COMMAND      USER         TYPE NODE   NAME
postgres     pgsql        IPv4 TCP    127.0.0.1:5432
interface    root         IPv4 TCP    127.0.0.1:53
ftpd.main    root         IPv4 TCP    10.0.202.7:21
gui          root         IPv4 TCP    10.0.202.7:80
gui          root         IPv4 TCP    10.0.202.7:443
ginetd       root         IPv4 TCP    10.0.202.7:22
java         root         IPv6 TCP    [::127.0.0.1]:18081
hermes       root         IPv4 TCP    10.0.202.7:25
hermes       root         IPv4 TCP    10.0.202.7:7025
api_serve    root         IPv4 TCP    10.0.202.7:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    10.0.202.7:6443
nginx        root         IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
nginx        nobody       IPv4 TCP    *:4431
java         root         IPv4 TCP    127.0.0.1:9999
```

NETSTAT

此實用程式顯示傳輸控制協定（傳入和傳出）的網路連線、路由表以及許多網路介面和網路協定統計資訊。

```
example.com> netstat

Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
```

Example of Option 1 (List of active sockets)

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 10.0.202.7.10275       10.0.201.4.6025        ESTABLISHED
tcp4       0      0 10.0.202.7.22          10.0.201.4.57759       ESTABLISHED
tcp4       0      0 10.0.202.7.10273       a96-17-177-18.deploy.static.akamaitechnologies.com.80
TIME_WAIT
tcp4       0      0 10.0.202.7.10260       10.0.201.5.443     ESTABLISHED
tcp4       0      0 10.0.202.7.10256       10.0.201.5.443     ESTABLISHED
```

Example of Option 2 (State of network interfaces)

```
Show the number of dropped packets? [N]> y

Name    Mtu Network       Address              Ipkts Ierrs Idrop     Ibytes    Opkts Oerrs
Obytes  Coll  Drop
Data 1    - 10.0.202.0    10.0.202.7        110624529     -     - 117062552515 122028093     -
30126949890     -     -
```

Example of Option 3 (Contents of routing tables)

```
Routing tables

Internet:
Destination        Gateway            Flags      Netif Expire
default            10.0.202.1         UGS         Data 1
10.0.202.0         link#2             U           Data 1
10.0.202.7         link#2             UHS         lo0
localhost.example. link#4             UH          lo0
```

Example of Option 4 (Size of the listen queues)

```
Current listen queue sizes (qlen/incqlen/maxqlen)
Proto Listen         Local Address
tcp4  0/0/50         localhost.exampl.9999
tcp4  0/0/50         10.0.202.7.7025
tcp4  0/0/50         10.0.202.7.25
tcp4  0/0/15         10.0.202.7.6443
tcp4  0/0/15         localhost.exampl.60001
tcp4  0/0/15         10.0.202.7.6080
tcp4  0/0/20         localhost.exampl.18081
tcp4  0/0/20         10.0.202.7.443
tcp4  0/0/20         10.0.202.7.80
tcp4  0/0/10         10.0.202.7.21
tcp4  0/0/10         10.0.202.7.22
tcp4  0/0/10         localhost.exampl.53
tcp4  0/0/208        localhost.exampl.5432
```

Example of Option 5 (Packet traffic information)

```
            input           nic1           output
   packets  errs idrops      bytes    packets  errs      bytes colls drops
        49     0      0       8116         55     0       7496     0     0
```

網路

diagnostic下的network子命令提供對其他選項的訪問。您可以使用此命令刷新所有與網路相關的快取、顯示ARP快取的內容、顯示NDP快取的內容（如果適用），並允許您使用SMTPING測試遠端SMTP連線。

```
example.com> diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> network


Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]>
```

ETHERCONFIG

其 etherconfig 命令允許您檢視和配置與介面、VLAN、環回介面、MTU大小以及接受或拒絕帶有組播地址的ARP應答有關的部分設定。

```
example.com> etherconfig


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

TRACEROUTE

顯示到遠端主機的網路路由。或者，您可以使用 traceroute6 命令（如果至少在一個介面上配置了IPv6地址）。

```
example.com> traceroute google.com
```

```
Press Ctrl-C to stop.
traceroute to google.com (216.58.194.206), 64 hops max, 40 byte packets
1 68.232.129.2 (68.232.129.2) 0.902 ms
68.232.129.3 (68.232.129.3) 0.786 ms 0.605 ms
2 139.138.24.10 (139.138.24.10) 0.888 ms 0.926 ms 1.092 ms
3 68.232.128.2 (68.232.128.2) 1.116 ms 0.780 ms 0.737 ms
4 139.138.24.42 (139.138.24.42) 0.703 ms
208.90.63.209 (208.90.63.209) 1.413 ms
139.138.24.42 (139.138.24.42) 1.219 ms
5 svl-edge-25.inet.qwest.net (63.150.59.25) 1.436 ms 1.223 ms 1.177 ms
6 snj-edge-04.inet.qwest.net (67.14.34.82) 1.838 ms 2.086 ms 1.740 ms
7 108.170.242.225 (108.170.242.225) 1.986 ms 1.992 ms
108.170.243.1 (108.170.243.1) 2.852 ms
8 108.170.242.225 (108.170.242.225) 2.097 ms
108.170.243.1 (108.170.243.1) 2.967 ms 2.812 ms
9 108.170.237.105 (108.170.237.105) 1.974 ms
sfo03s01-in-f14.1e100.net (216.58.194.206) 2.042 ms 1.882 ms
```

PING

Ping允許您使用IP地址或主機名測試主機可達性，並提供與通訊中可能的延遲和/或丟棄有關的統計資訊。

```
example.com> ping google.com

Press Ctrl-C to stop.
PING google.com (216.58.194.206): 56 data bytes
64 bytes from 216.58.194.206: icmp_seq=0 ttl=56 time=2.095 ms
64 bytes from 216.58.194.206: icmp_seq=1 ttl=56 time=1.824 ms
64 bytes from 216.58.194.206: icmp_seq=2 ttl=56 time=2.005 ms
64 bytes from 216.58.194.206: icmp_seq=3 ttl=56 time=1.939 ms
64 bytes from 216.58.194.206: icmp_seq=4 ttl=56 time=1.868 ms
64 bytes from 216.58.194.206: icmp_seq=5 ttl=56 time=1.963 ms

--- google.com ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.824/1.949/2.095/0.088 ms
```